ICS 35.040
L 80



中华人民共和国国家标准

GB/T 22080—2016/ISO/IEC 27001:2013
代替 GB/T 22080—2008

信息技术　安全技术
信息安全管理体系　要求

Information technology—Security techniques—Information security management systems—Requirements

（ISO/IEC 27001:2013,IDT）

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目 次

前言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22080—2008《信息技术安全技术信息安全管理体系要求》。

与 GB/T 22080—2008 相比，主要技术变化如下：

——结构变化见附录 NA；

——术语变化见附录 NB。

本标准使用翻译法等同采用 ISO/IEC 27001:2013《信息技术　安全技术　信息安全管理体系　要求》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009,IDT)

本标准做了下列编辑性修改：

——增加了资料性附录 NA；

——增加了资料性附录 NB。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、中电长城网际系统应用有限公司、中国信息安全认证中心、山东省标准化研究院、广州赛宝认证中心服务有限公司、北京江南天安科技有限公司、上海三零卫士信息安全有限公司、中国合格评定国家认可中心、北京时代新威信息技术有限公司、黑龙江电子信息产品监督检验院、浙江远望电子有限公司、杭州在信科技有限公司。

本标准主要起草人：上官晓丽、许玉娜、闵京华、尤其、公伟、卢列文、倪文静、王连强、陈冠直、于惊涛、付志高、赵英庆、卢普明、王曙光、虞仲华、韩硕祥、魏军、程瑜琦、孔祥林、邬敏华、李华、李阳。

本标准所代替标准的历次版本发布情况为：

——GB/T 22080—2008。

引　言

0.1 总则

本标准提供建立、实现、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略性决策。组织信息安全管理体系的建立和实现受组织的需要和目标、安全要求、组织所采用的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性、完整性和可用性,并为相关方树立风险得到充分管理的信心。

重要的是,信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中,并且在过程、信息系统和控制的设计中要考虑到信息安全。期望的是,信息安全管理体系的实现程度要与组织的需要相符合。

本标准可被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中所表述要求的顺序不反映各要求的重要性或暗示这些要求要予实现的顺序。条款编号仅为方便引用。

ISO/IEC 27000 描述了信息安全管理体系的概要和词汇,引用了信息安全管理体系标准族(包括 ISO/IEC 27003[2]、ISO/IEC 27004[3]、ISO/IEC 27005[4]),以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本标准应用 ISO/IEC 合并导则附录 SL 中定义的高层结构、相同条款标题、相同文本、通用术语和核心定义,因此维护了与其他采用附录 SL 的管理体系的标准具有兼容性。

附录 SL 中定义的通用途径对于选择运行单一管理体系来满足两个或更多管理体系标准要求的组织是有用的。

信息技术　安全技术　信息安全管理体系　要求

1　范围

本标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。

本标准规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本标准时，不能排除第 4 章到第 10 章中所规定的任何要求。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

3　术语和定义

ISO/IEC 27000 界定的术语和定义适用于本文件。

4　组织环境

4.1　理解组织及其环境

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

注：对这些事项的确定，参见 ISO 31000:2009[5]，5.3 中建立外部和内部环境的内容。

4.2　理解相关方的需求和期望

组织应确定：

a)　信息安全管理体系相关方；

b)　这些相关方与信息安全相关的要求。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3　确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a)　4.1 中提到的外部和内部事项；

b)　4.2 中提到的要求；

c)　组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。

4.4 信息安全管理体系

组织应按照本标准的要求，建立、实现、维护和持续改进信息安全管理体系。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：

a) 确保建立了信息安全策略和信息安全目标，并与组织战略方向一致；

b) 确保将信息安全管理体系要求整合到组织过程中；

c) 确保信息安全管理体系所需资源可用；

d) 沟通有效的信息安全管理及符合信息安全管理体系要求的重要性；

e) 确保信息安全管理体系达到预期结果；

f) 指导并支持相关人员为信息安全管理体系的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色，以证实他们的领导按角色应用于其责任范围。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a) 与组织意图相适宜；

b) 包括信息安全目标(见 6.2)或为设定信息安全目标提供框架；

c) 包括对满足适用的信息安全相关要求的承诺；

d) 包括对持续改进信息安全管理体系的承诺。

信息安全方针应：

e) 形成文件化信息并可用；

f) 在组织内得到沟通；

g) 适当时，对相关方可用。

5.3 组织的角色，责任和权限

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理层应分配责任和权限，以：

a) 确保信息安全管理体系符合本标准的要求；

b) 向最高管理者报告信息安全管理体系绩效。

注：最高管理层也可为组织内报告信息安全管理体系绩效，分配责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划信息安全管理体系时，组织应考虑 4.1 中提到的事项和 4.2 中提到的要求，并确定需要应对的风险和机会，以：

a) 确保信息安全管理体系可达到预期结果；

b） 预防或减少不良影响；

c） 达到持续改进。

组织应规划：

d） 应对这些风险和机会的措施；

e） 如何：

1） 将这些措施整合到信息安全管理体系过程中，并予以实现；

2） 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估过程，以：

a） 建立并维护信息安全风险准则，包括：

1） 风险接受准则；

2） 信息安全风险评估实施准则。

b） 确保反复的信息安全风险评估产生一致的、有效的和可比较的结果。

c） 识别信息安全风险：

1） 应用信息安全风险评估过程，以识别信息安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；

2） 识别风险责任人。

d） 分析信息安全风险：

1） 评估 6.1.2c) 1)中所识别的风险发生后，可能导致的潜在后果；

2） 评估 6.1.2c) 1)中所识别的风险实际发生的可能性；

3） 确定风险级别。

e） 评价信息安全风险：

1） 将风险分析结果与 6.1.2a)中建立的风险准则进行比较；

2） 为风险处置排序已分析风险的优先级。

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处置

组织应定义并应用信息安全风险处置过程，以：

a） 在考虑风险评估结果的基础上，选择适合的信息安全风险处置选项；

b） 确定实现已选的信息安全风险处置选项所必需的所有控制；

注 1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c） 将 6.1.3b)确定的控制与附录 A 中的控制进行比较，并验证没有忽略必要的控制；

注 2：附录 A 包含了控制目标和控制的综合列表。本标准用户可在附录 A 的指导下，确保没有遗漏必要的控制。

注 3：控制目标隐含在所选择的控制内。附录 A 所列的控制目标和控制并不是完备的，可能需要额外的控制目标和控制。

d） 制定一个适用性声明，包含必要的控制[见 6.1.3 b)和 c)]及其选择的合理性说明（无论该控制是否已实现），以及对附录 A 控制删减的合理性说明；

e） 制定正式的信息安全风险处置计划；

f） 获得风险责任人对信息安全风险处置计划以及对信息安全残余风险的接受的批准。

组织应保留有关信息安全风险处置过程的文件化信息。

注 4：本标准中的信息安全风险评估和处置过程与 ISO 31000[5] 中给出的原则和通用指南相匹配。

6.2 信息安全目标及其实现规划

组织应在相关职能和层级上建立信息安全目标。

信息安全目标应：

a） 与信息安全方针一致；

b） 可测量(如可行)；

c） 考虑适用的信息安全要求，以及风险评估和风险处置的结果；

d） 得到沟通；

e） 适当时更新。

组织应保留有关信息安全目标的文件化信息。

在规划如何达到信息安全目标时，组织应确定：

f） 要做什么；

g） 需要什么资源；

h） 由谁负责；

i） 什么时候完成；

j） 如何评价结果。

7 支持

7.1 资源

组织应确定并提供建立、实现、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

a） 确定在组织控制下从事会影响组织信息安全绩效的工作人员的必要能力；

b） 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c） 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d） 保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，例如针对现有雇员提供培训、指导或重新分配；雇佣或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

a） 信息安全方针；

b） 其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c） 不符合信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部的沟通需求，包括：

a） 沟通什么；

b） 何时沟通；

c） 与谁沟通；

d） 谁来沟通；

e） 影响沟通的过程。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a） 本标准要求的文件化信息；

b） 为信息安全管理体系的有效性，组织所确定的必要的文件化信息。

注：不同组织有关信息安全管理体系文件化信息的详略程度可以是不同的，这是由于：

1） 组织的规模及其活动、过程、产品和服务的类型；

2） 过程及其相互作用的复杂性；

3） 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a） 标识和描述（例如标题、日期、作者或引用编号）；

b） 格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）；

c） 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

信息安全管理体系及本标准所要求的文件化信息应得到控制，以确保：

a） 在需要的地点和时间，是可用的和适宜使用的；

b） 得到充分的保护（如避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，适用时，组织应强调以下活动：

c） 分发，访问，检索和使用；

d） 存储和保护，包括保持可读性；

e） 控制变更（例如版本控制）；

f） 保留和处理。

组织确定的为规划和运行信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

注：访问隐含着仅允许浏览文件化信息，或允许和授权浏览及更改文件化信息等决定。

8 运行

8.1 运行规划和控制

为了满足信息安全要求以及实现 6.1 中确定的措施，组织应规划、实现和控制所需要的过程。组织还应实现为达到 6.2 中确定的信息安全目标一系列计划。

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保外包过程是确定的和受控的。

8.2 信息安全风险评估

组织应考虑 6.1.2a）所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。

组织应保留信息安全风险评估结果的文件化信息。

8.3 信息安全风险处置

组织应实现信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应评价信息安全绩效以及信息安全管理体系的有效性。

组织应确定：

a) 需要被监视和测量的内容，包括信息安全过程和控制；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果；

注：所选的方法宜产生可比较和可再现的有效结果。

c) 何时应执行监视和测量；

d) 谁应监视和测量；

e) 何时应分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果。

组织应保留适当的文件化信息作为监视和测量结果的证据。

9.2 内部审核

组织应按计划的时间间隔进行内部审核，以提供信息，确定信息安全管理体系：

a) 是否符合：

  1) 组织自身对信息安全管理体系的要求；

  2) 本标准的要求。

b) 是否得到有效实现和维护。

组织应：

c) 规划、建立、实现和维护审核方案(一个或多个)，包括审核频次、方法、责任、规划要求和报告。审核方案应考虑相关过程的重要性和以往审核的结果。

d) 定义每次审核的审核准则和范围。

e) 选择审核员并实施审核，确保审核过程的客观性和公正性。

f) 确保将审核结果报告至相关管理层。

g) 保留文件化信息作为审核方案和审核结果的证据。

9.3 管理评审

最高管理层应按计划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a) 以往管理评审提出的措施的状态；

b) 与信息安全管理体系相关的外部和内部事项的变化；

c) 有关信息安全绩效的反馈，包括以下方面的趋势：

  1) 不符合和纠正措施；

  2) 监视和测量结果；

3） 审核结果；
4） 信息安全目标完成情况；

d） 相关方反馈；
e） 风险评估结果及风险处置计划的状态；
f） 持续改进的机会。

管理评审的输出应包括与持续改进机会相关的决定以及变更信息安全管理体系的任何需求。

组织应保留文件化信息作为管理评审结果的证据。

10 改进

10.1 不符合及纠正措施

当发生不符合时，组织应：

a） 对不符合做出反应，适用时：
   1） 采取措施，以控制并予以纠正；
   2） 处理后果；
b） 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：
   1） 评审不符合；
   2） 确定不符合的原因；
   3） 确定类似的不符合是否存在，或可能发生；
c） 实现任何需要的措施；
d） 评审任何所采取的纠正措施的有效性；
e） 必要时，对信息安全管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适合。

组织应保留文件化信息作为以下方面的证据：

f） 不符合的性质及所采取的任何后续措施；
g） 任何纠正措施的结果。

10.2 持续改进

组织应持续改进信息安全管理体系的适宜性、充分性和有效性。

附 录 A
（规范性附录）
参考控制目标和控制

表 A.1 所列的控制目标和控制是直接源自并与 GB/T 22081—2016[1]第 5 章～第 18 章相对应，并在 6.1.3 环境中被使用。

表 A.1 控制目标和控制

A.5 信息安全策略		
A.5.1 信息安全管理指导		
目标：依据业务要求和相关法律法规，为信息安全提供管理指导和支持		
A.5.1.1	信息安全策略	*控制* 信息安全策略集应被定义，由管理者批准，并发布、传达给所有员工和外部相关方。
A.5.1.2	信息安全策略的评审	*控制* 应按计划的时间间隔或当重大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。
A.6 信息安全组织		
A.6.1 内部组织		
目标：建立一个管理框架，以启动和控制组织内信息安全的实现和运行。		
A.6.1.1	信息安全的角色和责任	*控制* 所有的信息安全责任应予以定义和分配。
A.6.1.2	职责分离	*控制* 应分离冲突的职责及其责任范围，以减少未授权或无意的修改或者不当使用组织资产的机会。
A.6.1.3	与职能机构的联系	*控制* 应维护与相关职能机构的适当联系。
A.6.1.4	与特定相关方的联系	*控制* 应维护与特定相关方、其他专业安全论坛和专业协会的适当联系。
A.6.1.5	项目管理中的信息安全	*控制* 应关注项目管理中的信息安全问题，无论何种类型的项目。
A.6.2 移动设备和远程工作		
目标：确保移动设备远程工作及其使用的安全。		
A.6.2.1	移动设备策略	*控制* 应采用相应的策略及其支持性的安全措施以管理由于使用移动设备所带来的风险。
A.6.2.2	远程工作	*控制* 应实现相应的策略及其支持性的安全措施，以保护在远程工作地点上所访问的、处理的或存储的信息。

表 A.1（续）

A.7　人力资源安全		
A.7.1　任用前		
目标:确保员工和合同方理解其责任,并适合其角色		
A.7.1.1	审查	*控制* 应按照相关法律法规和道德规范,对所有任用候选者的背景进行验证核查,并与业务要求、访问信息的等级和察觉的风险相适宜
A.7.1.2	任用条款及条件	*控制* 应在员工和合同方的合同协议中声明他们和组织对信息安全的责任。
A.7.2　任用中		
目标:确保员工和合同方意识到并履行其信息安全责任。		
A.7.2.1	管理责任	*控制* 管理者应宜要求所有员工和合同方按照组织已建立的策略和规程应用信息安全。
A.7.2.2	信息安全意识、教育和培训	*控制* 组织所有员工和相关的合同方,应按其工作职能,接受适当的意识教育和培训,及组织策略及规程的定期更新的信息。
A.7.2.3	违规处理过程	*控制* 应有正式的、且已被传达的违规处理过程以对信息安全违规的员工采取措施。
A.7.3　任用的终止和变更		
目标:在任用变更或终止过程中保护组织的利益。		
A.7.3.1	任用终止或变更的责任	*控制* 应确定任用终止或变更后仍有效的信息安全责任及其职责,传达至员工或合同方并执行。
A.8　资产管理		
A.8.1　有关资产的责任		
目标:识别组织资产并定义适当的保护责任。		
A.8.1.1	资产清单	*控制* 应识别信息,以及与信息和信息处理设施相关的其他资产,并编制和维护这些资产的清单。
A.8.1.2	资产的所属关系	*控制* 应维护资产清单中资产的所属关系。
A.8.1.3	资产的可接受使用	*控制* 应识别可接受的信息使用规则,以及与信息和信息处理设施有关的资产的可接受的使用规则,形成文件并加以实现。
A.8.1.4	资产归还	*控制* 所有员工和外部用户在任用、合同或协议终止时,应归还其占用的所有组织资产。

表 A.1（续）

A.8.2　信息分级		
目标:确保信息按照其对组织的重要程度受到适当水平的保护。		
A.8.2.1	信息的分级	*控制* 信息应按照法律要求、价值、重要性及其对未授权泄露或修改的敏感性进行分级。
A.8.2.2	信息的标记	*控制* 应按照组织采用的信息分级方案,制定并实现一组适当的信息标记规程。
A.8.2.3	资产的处理	*控制* 应按照组织采用的信息分级方案,制定并实现资产处理规程。
A.8.3　介质处理		
目标:防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。		
A.8.3.1	移动介质的管理	*控制* 应按照组织采用的分级方案,实现移动介质管理规程。
A.8.3.2	介质的处置	*控制* 应使用正式的规程安全地处置不再需要的介质。
A.8.3.3	物理介质的转移	*控制* 包含信息的介质在运送中应受到保护,以防止未授权访问、不当使用或毁坏。
A.9　访问控制		
A.9.1　访问控制的业务要求		
目标:限制对信息和信息处理设施的访问。		
A.9.1.1	访问控制策略	*控制* 应基于业务和信息安全要求,建立访问控制策略,形成文件并进行评审。
A.9.1.2	网络和网络服务的访问	*控制* 应仅向用户提供他们已获专门授权使用的网络和网络服务的访问。
A.9.2　用户访问管理		
目标:确保授权用户对系统和服务的访问,并防止未授权的访问。		
A.9.2.1	用户注册和注销	*控制* 应实现正式的用户注册及注销过程,以便可分配访问权。
A.9.2.2	用户访问供给	*控制* 应对所有系统和服务的所有类型用户,实现一个正式的用户访问供给过程以分配或撤销访问权。
A.9.2.3	特许访问权管理	*控制* 应限制并控制特许访问权的分配和使用。
A.9.2.4	用户的秘密鉴别信息管理	*控制* 应通过正式的管理过程控制秘密鉴别信息的分配。

表 A.1（续）

A.9.2.5	用户访问权的评审	*控制* 资产拥有者应定期对用户的访问权进行评审。
A.9.2.6	访问权的移除或调整	*控制* 所有员工和外部用户对信息和信息处理设施的访问权在任用、合同或协议终止时，应予以移除，或在变更时予以调整。
A.9.3　用户责任		
目标：让用户承担保护其鉴别信息的责任。		
A.9.3.1	秘密鉴别信息的使用	*控制* 应要求用户遵循组织在使用秘密鉴别信息时的惯例。
A.9.4　系统和应用访问控制		
目标：防止对系统和应用的未授权访问。		
A.9.4.1	信息访问限制	*控制* 应按照访问控制策略限制对信息和应用系统功能的访问。
A.9.4.2	安全登录规程	*控制* 当访问控制策略要求时，应通过安全登录规程控制对系统和应用的访问。
A.9.4.3	口令管理系统	*控制* 口令管理系统应是交互式的，并应确保优质的口令。
A.9.4.4	特权实用程序的使用	*控制* 对于可能超越系统和应用控制的实用程序的使用应予以限制并严格控制。
A.9.4.5	程序源代码的访问控制	*控制* 应限制对程序源代码的访问。
A.10　密码		
A.10.1　密码控制		
目标：确保适当和有效地使用密码技术以保护信息的保密性、真实性和(或)完整性。		
A.10.1.1	密码控制的使用策略	*控制* 应开发和实现用于保护信息的密码控制使用策略。
A.10.1.2	密钥管理	*控制* 应制定和实现贯穿其全生命周期的密钥使用、保护和生存期策略。
A.11　物理和环境安全		
A.11.1　安全区域		
目标：防止对组织信息和信息处理设施的未授权物理访问、损坏和干扰。		
A.11.1.1	物理安全边界	*控制* 应定义和使用安全边界来保护包含敏感或关键信息和信息处理设施的区域。
A.11.1.2	物理入口控制	*控制* 安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。

表 A.1(续)

A.11.1.3	办公室、房间和设施的安全保护	*控制* 应为办公室、房间和设施设计并采取物理安全措施。
A.11.1.4	外部和环境威胁的安全防护	*控制* 应设计和应用物理保护以防自然灾害、恶意攻击和意外。
A.11.1.5	在安全区域工作	*控制* 应设计和应用安全区域工作规程。
A.11.1.6	交接区	*控制* 访问点(例如交接区)和未授权人员可进人的其他点应加以控制,如果可能,应与信息处理设施隔离,以避免未授权访问。
A.11.2 设备		
目标:防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。		
A.11.2.1	设备安置和保护	*控制* 应安置或保护设备,以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。
A.11.2.2	支持性设施	*控制* 应保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。
A.11.2.3	布缆安全	*控制* 应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听、干扰或损坏
A.11.2.4	设备维护	*控制* 设备应予以正确地维护,以确保其持续的可用性和完整性。
A.11.2.5	资产的移动	*控制* 设备、信息或软件在授权之前不应带出组织场所。
A.11.2.6	组织场所外的设备与资产安全	*控制* 应对组织场所外的资产采取安全措施,要考虑工作在组织场所外的不同风险
A.11.2.7	设备的安全处置或再利用	*控制* 包含储存介质的设备的所有部分应进行核查,以确保在处置或再利用之前,任何敏感信息和注册软件已被删除或安全的重写。
A.11.2.8	无人值守的用户设备	*控制* 用户应确保无人值守的用户设备有适当的保护。
A.11.2.9	清理桌面和屏幕策略	*控制* 应针对纸质和可移动存储介质,采取清理桌面策略;应针对信息处理设施,采用清理屏幕策略。
A.12 运行安全		
A.12.1 运行规程和责任		
目标:确保正确、安全的运行信息处理设施。		
A.12.1.1	文件化的操作规程	*控制* 操作规程应形成文件,并对所需用户可用。

表 A.1（续）

A.12.1.2	变更管理	*控制* 应控制影响信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。
A.12.1.3	容量管理	*控制* 应对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。
A.12.1.4	开发、测试和运行环境的分离	*控制* 应分离开发、测试和运行环境，以降低对运行环境未授权访问或变更的风险。
A.12.2　恶意软件防范		
目标：确保信息和信息处理设施防范恶意软件。		
A.12.2.1	恶意软件的控制	*控制* 应实现检测、预防和恢复控制以防范恶意软件，并结合适当的用户意识教育。
A.12.3　备份		
目标：防止数据丢失		
A.12.3.1	信息备份	*控制* 应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。
A.12.4　日志和监视		
目标：记录事态并生成证据。		
A.12.4.1	事态日志	*控制* 应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。
A.12.4.2	日志信息的保护	*控制* 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。
A.12.4.3	管理员和操作员日志	*控制* 系统管理员和系统操作员活动应记入日志，并对日志进行保护和定期评审。
A.12.4.4	时钟同步	*控制* 一个组织或安全域内的所有相关信息处理设施的时钟，应与单一一个基准的时间源同步。
A.12.5　运行软件控制		
目标：确保运行系统的完整性。		
A.12.5.1	运行系统的软件安装	*控制* 应实现运行系统软件安装控制规程。
A.12.6　技术方面的脆弱性管理		
目标：防止对技术脆弱性的利用。		

表 A.1（续）

A.12.6.1	技术方面脆弱性的管理	*控制* 应及时获取在用的信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。
A.12.6.2	软件安装限制	*控制* 应建立并实现控制用户安装软件的规则。
A.12.7　信息系统审计的考虑		
目标：使审计活动对运行系统的影响最小化。		
A.12.7.1	信息系统审计的控制	*控制* 涉及运行系统验证的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化业务过程的中断。
A.13　通信安全		
A.13.1　网络安全管理		
目标：确保网络中的信息及其支持性的信息处理设施得到保护。		
A.13.1.1	网络控制	*控制* 应管理和控制网络以保护系统和应用中的信息。
A.13.1.2	网络服务的安全	*控制* 所有网络服务的安全机制、服务级别和管理要求应予以确定并包括在网络服务协议中，无论这些服务是由内部提供的还是外包的。
A.13.1.3	网络中的隔离	*控制* 应在网络中隔离信息服务、用户及信息系统。
A.13.2　信息传输		
目标：维护在组织内及与外部实体间传输信息的安全。		
A.13.2.1	信息传输策略和规程	*控制* 应有正式的传输策略、规程和控制，以保护通过使用各种类型通信设施进行的信息传输。
A.13.2.2	信息传输协议	*控制* 协议应解决组织与外部方之间业务信息的安全传输。
A.13.2.3	电子消息发送	*控制* 应适当保护包含在电子消息发送中的信息。
A.13.2.4	保密或不泄露协议	*控制* 应识别、定期评审和文件化反映组织信息保护需要的保密性或不泄露协议的要求。
A.14　系统获取、开发和维护		
A.14.1　信息系统的安全要求		
目标：确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求		
A.14.1.1	信息安全要求分析和说明	*控制* 新建信息系统或增强现有信息系统的要求中应包括信息安全相关要求。

表 A.1（续）

A.14.1.2	公共网络上应用服务的安全保护	*控制* 应保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。
A.14.1.3	应用服务事务的保护	*控制* 应保护应用服务事务中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放。
A.14.2　开发和支持过程中的安全		
目标：确保信息安全在信息系统开发生命周期中得到设计和实现。		
A.14.2.1	安全的开发策略	*控制* 针对组织内的开发，应建立软件和系统开发规则并应用。
A.14.2.2	系统变更控制规程	*控制* 应使用正式的变更控制规程来控制开发生命周期内的系统变更。
A.14.2.3	运行平台变更后对应用的技术评审	*控制* 当运行平台发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。
A.14.2.4	软件包变更的限制	*控制* 应不鼓励对软件包进行修改，仅限于必要的变更，且对所有变更加以严格控制
A.14.2.5	系统安全工程原则	*控制* 应建立、文件化和维护系统安全工程原则，并应用到任何信息系统实现工作中
A.14.2.6	安全的开发环境	*控制* 组织应针对覆盖系统开发生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。
A.14.2.7	外包开发	*控制* 组织应督导和监视外包系统开发活动
A.14.2.8	系统安全测试	*控制* 应在开发过程中进行安全功能测试。
A.14.2.9	系统验收测试	*控制* 应建立对新的信息系统、升级及新版本的验收测试方案和相关准则。
A.14.3　测试数据		
目标：确保用于测试的数据得到保护。		
A.14.3.1	测试数据的保护	*控制* 测试数据应认真地加以选择、保护和控制。
A.15　供应商关系		
A.15.1　供应商关系中的信息安全		
目标：确保供应商可访问的组织资产得到保护。		
A.15.1.1	供应商关系的信息安全策略	*控制* 为降低供应商访问组织资产的相关风险，应与供应商就信息安全要求达成一致，并形成文件

表 A.1(续)

A.15.1.2	在供应商协议中强调安全	*控制* 应与每个可能访问、处理、存储、传递组织信息或为组织信息提供IT基础设施组件的供应商建立所有相关的信息安全要求,并达成一致。
A.15.1.3	信息与通信技术供应链	*控制* 供应商协议应包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。
A.15.2 供应商服务交付管理		
目标:维护与供应商协议一致的信息安全和服务交付的商定级别。		
A.15.2.1	供应商服务的监视和评审	*控制* 组织应定期监视、评审和审核供应商服务交付。
A.15.2.2	供应商服务的变更管理	*控制* 应管理供应商所提供服务的变更,包括维护和改进现有的信息安全策略、规程和控制,管理应考虑变更涉及到的业务信息、系统和过程的关键程度及风险的再评估。
A.16 信息安全事件管理		
A.16.1 信息安全事件的管理和改进		
目标:确保采用一致和有效的方法对信息安全事件进行管理,包括对安全事态和弱点的沟通。		
A.16.1.1	责任和规程	*控制* 应建立管理责任和规程,以确保快速、有效和有序地响应信息安全事件。
A.16.1.2	报告信息安全事态	*控制* 应通过适当的管理渠道尽快地报告信息安全事态。
A.16.1.3	报告信息安全弱点	*控制* 应要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中的信息安全弱点。
A.16.1.4	信息安全事态的评估和决策	*控制* 应评估信息安全事态并决定其是否属于信息安全事件。
A.16.1.5	信息安全事件的响应	*控制* 应按照文件化的规程响应信息安全事件。
A.16.1.6	从信息安全事件中学习	*控制* 应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。
A.16.1.7	证据的收集	*控制* 组织应确定和应用规程来识别、收集、获取和保存可用作证据的信息。
A.17 业务连续性管理的信息安全方面		
A.17.1 信息安全的连续性		
目标:应将信息安全连续性纳入组织业务连续性管理之中。		

表 A.1（续）

A.17.1.1	规划信息安全连续性	*控制* 组织应确定在不利情况(如危机或灾难)下,对信息安全及信息安全管理连续性的要求。
A.17.1.2	实现信息安全连续性	*控制* 组织应建立、文件化、实现并维护过程、规程和控制,以确保在不利情况下信息安全连续性达到要求的级别。
A.17.1.3	验证、评审和评价信息安全连续性	*控制* 组织应定期验证已建立和实现的信息安全连续性控制,以确保这些控制在不利情况下是正当和有效的。
A.17.2　冗余		
目标:确保信息处理设施的可用性。		
A.17.2.1	信息处理设施的可用性	*控制* 信息处理设施应当实现冗余,以满足可用性要求。
A.18　符合性		
A.18.1　符合法律和合同要求		
目标:避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。		
A.18.1.1	适用的法律和合同要求的识别	*控制* 对每一个信息系统和组织而言,所有相关的法律、法规、规章和合同要求,以及为满足这些要求组织所采用的方法,应加以明确地定义、形成文件并保持更新。
A.18.1.2	知识产权	*控制* 应实现适当的规程,以确保在使用具有知识产权的材料和具有所有权的软件产品时,符合法律、法规和合同的要求。
A.18.1.3	记录的保护	*控制* 应根据法律、法规、规章、合同和业务要求,对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。
A.18.1.4	隐私和个人可识别信息保护	*控制* 应依照相关的法律、法规和合同条款的要求,以确保隐私和个人可识别信息得到保护。
A.18.1.5	密码控制规则	*控制* 密码控制的使用应遵从所有相关的协议、法律和法规。
A.18.2　信息安全评审		
目标:确保依据组织策略和规程来实现和运行信息安全。		
A.18.2.1	信息安全的独立评审	*控制* 应按计划的时间间隔或在重大变化发生时,对组织的信息安全管理方法及其实现(如信息安全的控制目标、控制、策略、过程和规程)进行独立评审。
A.18.2.2	符合安全策略和标准	*控制* 管理者应定期评审其责任范围内的信息处理和规程与适当的安全策略、标准和任何其他安全要求的符合性。
A.18.2.3	技术符合性评审	*控制* 应定期评审信息系统与组织的信息安全策略和标准的符合性。

附 录 NA
（资料性附录）
GB/T 22080—2016 与 GB/T 22080—2008 版对比

表 NA.1 GB/T 22080—2016 与 GB/T 22080—2008 版对比表

GB/T 22080—2016	GB/T 22080—2008
4 组织环境	
4.1 理解组织及其环境	8.3 预防措施
4.2 理解相关方的需求和期望	5.2.1 资源提供 7.3 评审输出
4.3 确定信息安全管理体系范围	4.2.1 建立 ISMS 4.2.3 监视和评审 ISMS 4.3.1 总则 4.3.2 文件控制
4.4 信息安全管理体系	4.1 总要求 5.2.1 资源提供
5 领导	
5.1 领导和承诺	4.2.1 建立 ISMS 5.1 管理承诺
5.2 方针	4.2.1 资源提供 4.3.2 总则 5.1 管理承诺
5.3 组织的角色，责任和权限	5.1 管理承诺 4.3.3 记录控制 6ISMS 内部审核
6 规划	
6.1 应对风险和机会的措施	
6.1.1 总则	4.2.1 建立 ISMS 8.3 预防措施
6.1.2 信息安全风险评估	4.2.1 建立 ISMS 5.1 管理承诺
6.1.3 信息安全风险处置	4.2.1 建立 ISMS 4.2.2 实施和运行 ISMS
6.2 信息安全目标及其实现规划	4.2.3 监视和评审 ISMS 4.3.1 总则 5.1 管理承诺
7 支持	
7.1 资源	4.2.2 实施和运行 ISMS 4.2.1 建立 ISMS

表 NA.1（续）

GB/T 22080—2016	GB/T 22080—2008
7.2 能力	5.2.2 培训、意识和能力
7.3 意识	4.2.2 实施和运行 ISMS 5.1 管理承诺 5.2.2 培训、意识和能力
7.4 沟通	4.2.4 保持和改进 ISMS 5.1 管理承诺
7.5 文件化信息	
7.5.1 总则	4.3.1 总则
7.5.2 创建和更新	4.3.2 文件控制 4.3.3 记录控制
7.5.3 文件化信息的控制	4.3.2 文件控制 4.3.3 记录控制
8 运行	
8.1 运行规划和控制	4.2.2 实施和运行 ISMS 4.3.3 记录控制 8.3 预防措施
8.2 信息安全风险评估	4.2.3 监视和评审 ISMS 4.3.1 总则
8.3 信息安全风险处置	4.2.2 实施和运行 ISMS 4.3.3 记录控制
9 绩效评价	
9.1 监视、测量、分析和评价	4.2.2 实施和运行 ISMS 4.2.3 监视和评审 ISMS
9.2 内部审核	4.2.3 监视和评审 ISMS 4.3.1 总则 4.3.3 记录控制 6ISMS 内部审核
9.3 管理评审	4.2.3 监视和评审 ISMS 5.1 管理承诺 5.2.1 资源提供 7.1 总则 7.2 评审输入 7.3 评审输出
10 改进	
10.1 不符合及纠正措施	4.2.4 保持和改进 ISMS 8.2 纠正措施 8.3 预防措施
10.2 持续改进	4.2.4 保持和改进 ISMS 5.2.1 资源提供 8.1 持续改进

附 录 NB
（资料性附录）
GB/T 22080—2016 与 GB/T 22080—2008 主要关键词变化

1 Control “控制措施”改为“控制”。

2 Implement “实施”改为“实现”

3 Maintain “保持”改为“维护”

4 asset owner “资产责任人”改为“资产拥有者”

参 考 文 献

[1] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[2] ISO/IEC 27003 信息技术 安全技术 信息安全管理体系实施指南
[3] ISO/IEC 27004 信息技术 安全技术 信息安全管理 测量
[4] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理
[5] ISO 31000:2009 风险管理 原则和指南
[6] ISO/IEC 导则 第一部分,ISO 综合补充 ISO 具体规程,2012